NIST Special Publication 800-xx

D R A F T

Guidelines to Federal Organizations on Assessing Information Technology (IT) Security Programs

Recommendations of the National Institute of Standards and Technology

U.S. DEPARTMENT OF COMMERCE

Technology Administration

National Institute of Standards and Technology

Frances H. Nielsen

COMPUTER SECURITY

D R A F T

(7-11-00)

Comments may be sent to assessment@nist.gov *and are requested by August 25, 2000.*

Guidelines to Federal Organizations on Information Technology Security Assessments

Recommendations of the National Institute of Standards and Technology

Purpose

This document provides guidelines for the assessment of Federal information system security programs. NIST's advice is provided in the context of other recommendations and guidelines for securing Federal information systems.

Authority

This document has been developed by NIST in furtherance of its statutory responsibilities (under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3(a)(5)). This is not a guideline within the meaning of (15 U.S.C. 278 g-3(a)(3)).

These recommendations are for use by Federal organizations which process sensitive information.[1]

The recommendations herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon Federal agencies by the Secretary of Commerce under his statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

Background

These guidelines provide advice to agencies *for sensitive (i.e., non-national security) unclassified systems*.

[1] Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive information:" *any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy*.

Information technology (IT) security is a fundamental management responsibility. To carry out that responsibility, measures and mechanisms are needed to determine how well an organization is protecting its IT systems and the information they possess (i.e., the health of IT security in an organization) and to demonstrate whether the security program is adequate and agile enough to meet the organizational mission and its goals. Measuring IT security is difficult because many measures may apply.

A first step to comparing and improving security programs is achieving a consistent, high-level picture. Tools, guidelines, and standards for measuring individual application systems exist; however, an effective management level metric for security is needed. To that end, the Chief Information Officer's Council Security Privacy and Critical Infrastructure Committee initiated a project to create a framework for assessing Federal security management programs. Called the Information Technology Security Assessment Framework, the Council issued version one of the document in July 2000.

The NIST-developed Framework responds to the recognized need to improve the security of Federal information resources and systems. The Framework identifies five levels of achievement for IT security programs. It is one of several tools organizations may use to determine the health of their security programs. Like taking a patient's pulse, the assessment results will give IT security managers and others, such as heads of departments, a starting point for continued examination and improvement. The assessment will provide clues about what security areas are covered and what concerns may need to be addressed.

The criteria described in the Framework are well-established measures based on existing statutes (e.g., the Computer Security Act of 1987), Federal guidance (e.g., OMB Circular A-130), audit questions (e.g., the Federal Information System Computer Auditing Manual), and recommended security practices (e.g., NIST Special Publications). The Framework provides a means for consistent and effective application of existing policy and guidance.

This recommendation provides guidelines for understanding and using an assessment model, in particular, the Information Technology Security Assessment Framework, endorsed by the Federal CIO Council.

Guidelines

1. **Federal departments and agencies should use an assessment process model, such as the Information Technology Security Assessment Framework, to help build a strong computer security program.**

A model that enumerates the components of a mature security program can be helpful in building a strong IT security program, key to good IT security. The building blocks of the Assessment Framework focus on the fundamentals of a security program: a program plan, the high level policy, and detailed implementation procedures. Federal departments

and agencies that follow the Framework in building IT security programs will address the basics for a strong program.

An assessment model is useful in understanding the current state of IT security programs. If improvements are needed, it is important to know the starting point. The IT Security Assessment Framework facilitates a state-of-the-security-program assessment by providing a step-wise approach to assessment. This approach is predictably more comprehensive than other approaches. It is expected that the results of its use will be more reliable than a haphazard, hit-or-miss scrutiny. Using the Framework, examination is more thorough and is consistently applied.

2. Federal departments and agencies should review the Framework provided in the appendix and understand the benefits and limitations of its use.

Many benefits accrue from using an agreed-upon framework across the Federal government. A primary benefit is that consistent comparisons can be made among Departments, Agencies, and programs within these organizations. The meaning and rationale for each measurement can be well-understood and can be communicated effectively. This is equally true whether the measurement is between peer-to-peer organizations (e.g., agency-to-agency comparisons), across organizational units (e.g., downwards to subordinate agency components), or for oversight purposes (e.g., Inspectors General).

Another benefit is that the approach proposed by the Framework is relatively simplistic, so it may be applied easily and frequently. Essentially the Framework can provide a "snapshot" view of an agency's security posture. Any missing security controls as well as problems, holes, or concerns can be spotted and addressed quickly. While not replacing a thorough, detailed security review, the snapshot assessment indicates where improvements are most needed. The assessment can help prioritize security activities.

The criteria presented in the Framework can apply to entire programs or program components.

The Framework supports immediate implementation. Agencies can take steps now to assess and to improve their programs.

The Framework does not provide detailed security checklists. Until more detailed measures are defined, the Framework covers only a broad management view of the security program.

The Framework is a starting point to building strong IT security programs. After the program is assessed, actions to maintain and/or improve the program must follow. Follow-on activities, such as promulgating and implementing any missing IT security procedures, are vital to achieving effective programs.

3. Federal departments and agencies should assess (or have assessed by others) their current program against the Framework.

Reviews are opportunities to highlight and endorse strengths and to take corrective actions on any weaknesses. Agencies should thoroughly and regularly review their management, operational, and technical security controls. Direction from OMB (Circular A-130) indicates that a review should be completed every three years or whenever a significant change occurs.

Agencies may use the Framework for self-assessments or the assessment may be performed by outside consultants and experts. The Framework's emphasis on measuring "foundation" activities -- such as the completeness of security policies, plans, and procedures -- makes implementation easier to achieve while providing a guide for an evolution to more robust and effective security controls.

4. Federal agencies should identify a target assessment level.

The Framework identifies five levels of assessment. Each of these levels contains positive characteristics. Each higher level builds on the strengths of the levels below it. Each higher level adds complexity and cost while addressing different security concerns. The topmost level is not necessarily the most appropriate, nor will it be cost-effective, for every agency and every agency program. The Framework does not endorse, and NIST does not endorse, a one-level-fits-all answer to security assessment.

Agencies should use a risk assessment approach, as required by OMB Circular A-130, to understand the threat and risk environment that applies to the information they manage. Based on this threat and risk environment, agencies should use the IT Security Assessment Framework to identify a target level.

A match between acceptable risk and security coverage can identify a goal level. The overall goal level for an agency may not be the same goal level of specific agency applications. For example, an agency's mission critical programs may likely have a higher goal level than other agency programs.

5. **If Federal departments and agencies are not at their target assessment level, they should develop and implement a plan to achieve that level.**

Using the framework to assess the health of security programs is merely the first step. For healthy programs, the framework can be applied continually to maintain that healthy state. For programs that need to be improved, agencies need a plan for improvement. The plan should be comprehensive and implement steps to achieve the target assessment level.

Supplemental Information

Appendix I:

Draft Information Security Assessment Framework